Defense Information Systems Agency

A Combat Support Agency

An Overview of the VTF DIACAP Process

DISN Video Services
September 21, 2009

DISA

A Combat Support Agency

How to Get Your Video Teleconferencing Facility (VTF) Accredited

DISN Video Services (NS5)

DISA
A Combat Support Agency

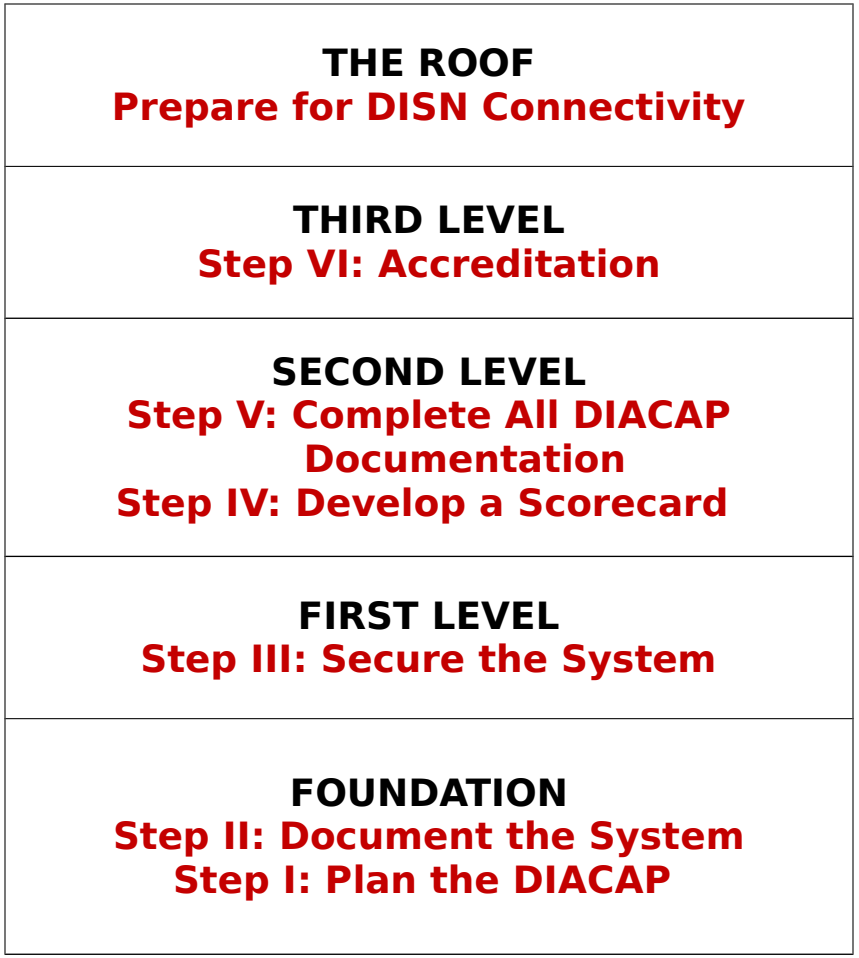
Introduction

- Accrediting your Video Teleconference Facility (VTF) helps protect the information that is vital to your mission. Thus, the VTF DIACAP is essential.
- You are free to follow the VTF DIACAP Process that works best for your organization.
- Today's presentation outlines our process for accrediting a VTF.
- The steps in this process cover the first three phases of DIACAP process as outlined in DoDI 8510.01.
- After completing this process, accreditation must be maintained (8510.01 DIACAP Phase IV).
- Links to all of the documents mentioned are at the end of this presentation.

DISA
A Combat Support Agency

The VTF DIACAP Process

- In some ways, following the VTF DIACAP Process is like constructing a secure, stable three-story building.
- Here is a simple "blueprint".
- First, ensure that you have a strong foundation to build upon.
- Then you can build the next levels on top of each other.



DISA

A Combat Support Agency

Step I: Plan the DIACAP

- **Consult your organization's Designated Accrediting Authority (DAA) and Certifying Authority (CA) about their C&A and information assurance (IA) control validation process. Follow their directions.**
- **If you cannot reach your DAA, then talk with your DAA representative.**
- **If your VTF has a current DITSCAP accreditation, develop a strategy and schedule for transitioning to DIACAP, achieving compliance with 8500.2 baseline IA controls, satisfying the DIACAP Annual Review, and meeting the reporting requirements of FISMA.**
  - **DISA has a DIACAP Transition Plan template that you can complete if your DAA requests one.**
- **Plan and schedule your DIACAP project.**
  - **Schedule security tests, etc.**
  - **Plan to meet your DAA's DIACAP package submission deadline**

DISA
A Combat Support Agency

Step I, Continued: MAC & CL

- **Decide the Mission Assurance Category (MAC) & Confidentiality Level (CL) for your VTF.**
  - **MAC I: High integrity, High availability**
    - **Cannot go down without having a significant impact on your mission.**
  - **MAC II: High integrity, Medium availability**
    - **Can go down for up to 24 hours without having a significant impact on your mission.**
  - **MAC III: Basic integrity, Basic availability**
    - **Can go down for up to 5 days without having a significant impact on your mission.**

DISA

A Combat Support Agency

Step I, Continued: MAC

- Mission Assurance Category I (MAC I)
  - **Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.**
- Mission Assurance Category II (MAC II)
  - **Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.**
- Mission Assurance Category III (MAC III)
  - **Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.**

DISA
A Combat Support Agency

Step I, Continued: CL

- The confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless).
- The Department of Defense has three defined confidentiality levels:
  - Classified
  - Sensitive
  - Public

DISA
A Combat Support Agency

Step I, Continued: IA Record Type & Criticality

- **Assign IA Record Type**
  - **AIS Application, Enclave, Outsourced IT-Based Process, or Platform IT Interconnection**
- **Assign Mission Criticality**
  - **Mission critical (MC), mission essential (ME), or mission support (MS)**

DISA

A Combat Support Agency

Step I, Type of C&A

- **Decide on the type of C&A you will conduct.**
  - **Type accreditation**
  - **Stand-alone IS accreditation**
- **The type accreditation is the official authorization to employ identical copies of a system in specified environments. This form of C&A allows a single DIACAP package (i.e., SIP, DIP, supporting documentation for certification, DIACAP Scorecard, and IT Security POA&M (if required)) to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location.**
  - **Automated Information System (AIS) applications accreditations are type accreditations.**
  - **Stand-alone IS and demilitarized zone (DMZ) accreditations may also be type accreditations.**

DISA

A Combat Support Agency

Step I, Type of C&A, Continued

- **Stand-alone ISs are treated as special types of enclaves that are not interconnected to any other network.**
- **Stand-alone systems do not transmit, receive, route, or interchange information outside of the system's accreditation boundary.**
- **IA requirements for a stand-alone system are determined by its MAC and classification or sensitivity and need-to-know just as for other DoD ISs.**
- **Stand-alone systems must always be clearly identified as such on the IT Security POA&M, the SIP, and the DIACAP Scorecard. Because of the unique architecture of a stand-alone system, certain IA controls do not pose a risk to the system as a result of their non-implementation and thus are considered NA.**

DISA
A Combat Support Agency

Step II: Document the System

- **Register your system with your DoD component IA program.**
  - **Complete your System Identification Profile (SIP)**
    - **The SIP is generated during the registration process and becomes part of the DIACAP package for the IS.**
- **Ensure that all of your system's documentation is complete and up-to-date.**
  - **Accreditation boundary, system architecture, & hardware/software inventory**
    - **Guidance and templates are on the VTF DIACAP Web Site.**
  - **IA controls**
    - **Initiate DIACAP Implementation Plan (DIP)**
  - **Other system documentation as needed.**

DISA
A Combat Support Agency

Step II, Continued: Inherited Controls

- **Inheritance refers to situations where IA controls along with their validation results and compliance status are shared by two or more systems for the purposes of C&A.**
- **Through inheritance, an existing IA control and its compliance status extends from an originating information system (IS) to a receiving IS.**
- **The general rule is that if a control that is applied to your VTF is being provided by an accredited resource that is not within your system's accreditation boundary, that control can be considered inherited.**
- **On the other hand, if a control is provided by resources that are within your VTF accreditation boundary, or if the external resource that is providing the control does not have a current, valid accreditation, then it can NOT be inherited.**

DISA
A Combat Support Agency

Step III: Secure the System

- **Your foundation is built. Now here is the first level of your building.**
- **Execute the DIACAP Implementation Plan**
- **Assess information assurance posture**
  - **Compliance to applicable STIGs is critical to successful VTF deployment.**
- **Which STIGs you need depends on what is inside the accreditation boundary of your VTF.**
- **Your DAA might require additional IA control validation procedures.**

THE ROOF Prepare for DISN Connectivity
THIRD LEVEL Step VI: Accreditation
SECOND LEVEL Step V: Complete All DIACAP Documentation Step IV: Develop a Scorecard
FIRST LEVEL Step III: Secure the System
FOUNDATION Step II: Document the System Step I: Plan the DIACAP

DISA
A Combat Support Agency

Step III, STIGs for ISDN VTF

- **We recommend that assessments are conducted utilizing the following STIG Security Checklists, as appropriate:**
  - For a VTF that utilizes only dial-up:
    - **IA Control Checklist**
      - **Use the IA Control Checklist with the proper IA control baseline for your VTF (based on the documented MAC & CL for your VTF).**
    - **Video Teleconference (VTC) Checklist**
      - **This checklist specifies which requirements are for IP and/or ISDN.**
    - **DoD Telecommunications & Defense Switched Network (DSN) Checklist**

DISA
A Combat Support Agency

Step III, STIGs for IP & ISDN VTF

- For a VTF that utilizes IP or both ISDN and/or IP:
  - **IA Control Checklist**
    - **Use the IA Control Checklist with the proper IA control baseline for your VTF (based on the documented MAC & CL for your VTF).**
  - **Video Teleconference (VTC) Checklist**
    - **This checklist specifies which requirements are for IP and/or ISDN.**
  - **Network Security Checklist – Firewall**
  - **Network Security Checklist – General Infrastructure Router**
  - **Network Security Checklist – Intrusion Detection System (IDS)**
  - **Network Security Checklist – Network Policy**
  - **DoD Telecommunications & Defense Switched Network (DSN) Checklist**
    - **Use only if you have Dial-up as well as IP.**

DISA
A Combat Support Agency

Step III, Vulnerability Management

- After you conduct the security assessments, you should create a POA&M and work to close as many vulnerabilities as possible.
- According to DoDI 8510.01p, page 18:
  - CAT I weaknesses shall be corrected before an ATO is granted.
  - CAT II weaknesses shall be corrected or satisfactorily mitigated before an ATO can be granted.
  - CAT III weaknesses will not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.
- Depending on the criticality of the mission, and your DAA's discretion, DoDI 8510.01p does offer some flexibility concerning CAT I and CAT II vulnerabilities.
  - For further guidance, consult your CA and DoDI 8510.01p.

Step IV: Develop DIACAP Scorecard

A Combat Support Agency

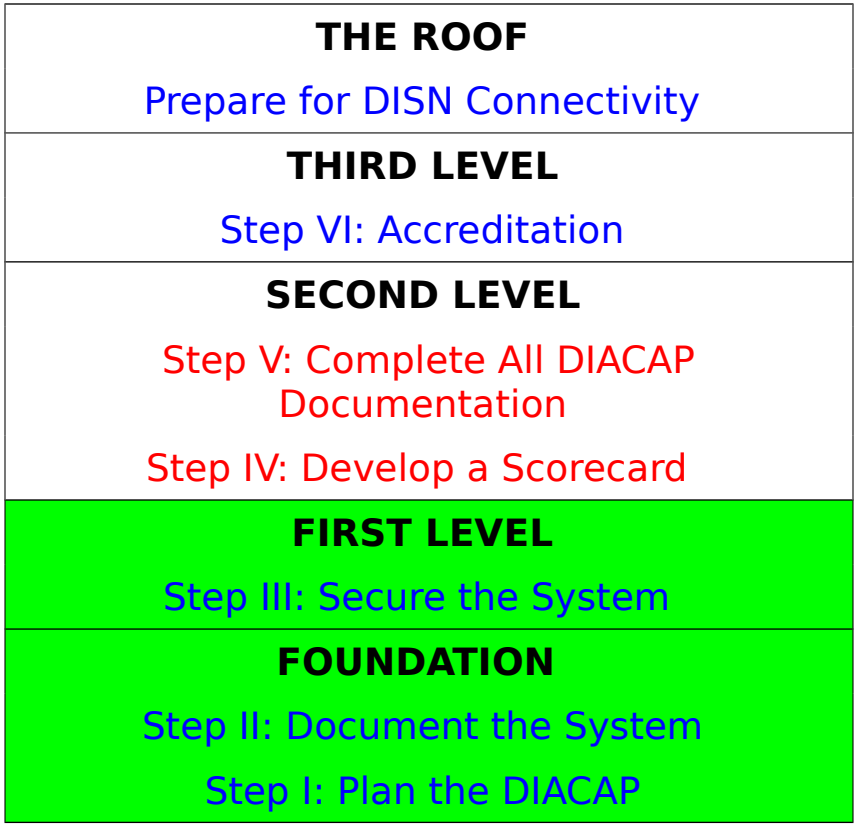
- **You have planned your DIACAP. You are following your DAA's advice. Your system documentation is up-to-date. You have completed the appropriate security assessments. You got your CATs in order.**
- **Now, in Step 4, translate assessment results into a DIACAP Scorecard.**
  - **The VTF Scorecard Matrix and instructions are on the VTF DIACAP Web site.**

THE ROOF
Prepare for DISN Connectivity
THIRD LEVEL
Step VI: Accreditation
SECOND LEVEL
Step V: Complete All DIACAP Documentation
Step IV: Develop a Scorecard
FIRST LEVEL
Step III: Secure the System
FOUNDATION
Step II: Document the System
Step I: Plan the DIACAP

Step V: Complete DIACAP Documents

A Combat Support Agency

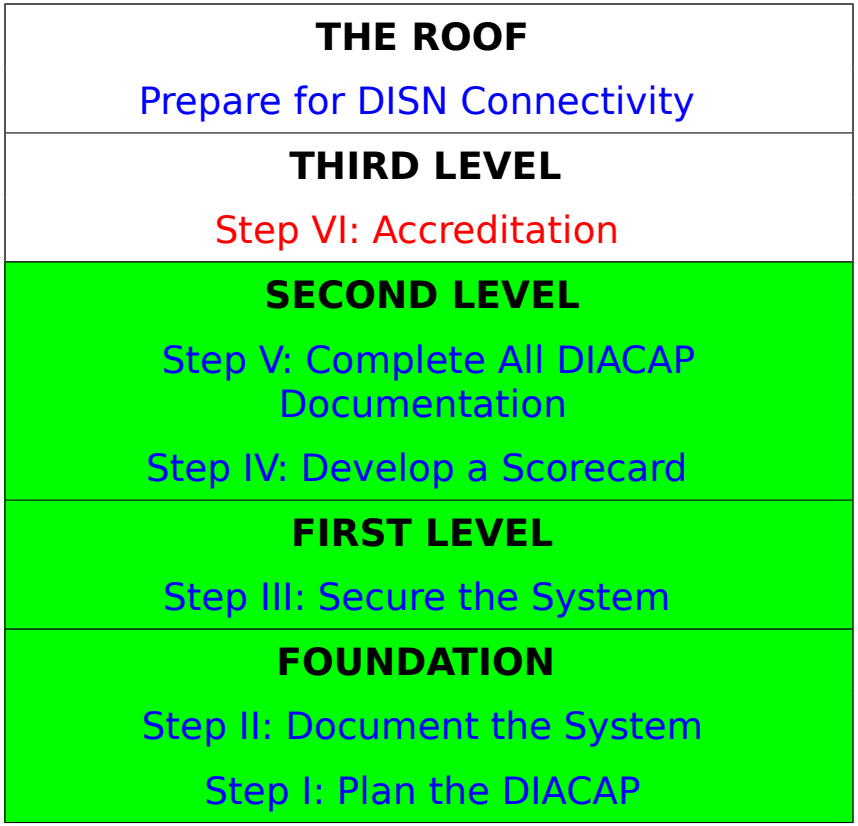
- **Now the security assessment results are in your Scorecard.**
- **Complete all the DIACAP documents requested by your DAA and submit them to your CA in accordance with your organization's requirements.**
- **Your DAA decides whether you need anything more than the DIACAP Executive Package.**
- **DISA provides several DIACAP templates that you may use on your own or within your organization.**



A Combat Support Agency

Step VI: Accredit the System

- **Your CA will make a certification recommendation to your DAA based on the DIACAP package that you submitted.**
- **Then depending on your organization, it could take a well over a month to get the accreditation decision from your DAA.**
- **Your DAA will convey the accreditation decision by signing a printed copy of the DIACAP Scorecard for your VTF.**
- **How do all of these VTF DIACAP Process steps compare to the DIACAP process outlined in 8510.01?**
- **The activities are basically the same.**



8510.01 & the VTF DIACAP Steps

A Combat Support Agency

8510.01 DIACAP Phases	8510.01 DIACAP Activities	VTF DIACAP	VTF DIACAP Activities
	Register IS with DoD component IA program		
		Step I	**Coordinate DIACAP Activities with Your DAA & CA**
		Step I	**Plan and Schedule DIACAP Activities**
	Assemble DIACAP Team	Step I	**Assemble DIACAP Team**
	Assign MAC, CL, IS type, & IA controls	Step I	**Assign MAC & CL, IA Record Type, Mission Criticality, C&A Type, & IA Controls**
		Step II	**Register System with DoD Component IA Program**
		Step II	**Document IS Accreditation Boundary, Architecture, & Hardware/Software Inventory**
	Initiate DIACAP Implementation Plan	Step II	**Initiate DIACAP Implementation Plan**
	Execute DIACAP Implementation Plan	Step III	**Execute DIACAP Implementation Plan**
	Conduct Validation Activities (DIACAP IA Control Validation Procedures)	Step III	**Conduct Validation Activities (DISA STIGs)**
Phase I	**Prepare POA&M**	Step III	**Prepare POA&M**
		Step III	**Fix/Mitigate Detected Vulnerabilities**
	Compile Validation Results in DIACAP Scorecard	Step III	**Compile Validation Results in DIACAP Scorecard (Scorecard Matrix)**
		Step IV	**Complete All DIACAP Documents (Artifacts, etc)**
Phase II	**Make Certification Determination**	Step V	**Make Certification Determination**
Phase III	**Issue Accreditation Decision**	Step VI	**Issue Accreditation Decision**
	Maintain Situational Awareness (Review of IA Controls must occur at least annually)	Step VI	**Maintain Situational Awareness (Review of IA Controls Must Occur at Least Annually)**
	Maintain IA Posture		**Maintain IA Posture**
Phase IV	**Initiate Re-Accreditation**		**Initiate Re-Accreditation**
Phase V	**Retire System**		**Retire System**

DISA

A Combat Support Agency

Prepare for DISN Connectivity

- **Once your VTF obtains an Authorization to Operate (ATO) or an Interim Authorization to Operate (IATO), you will need to go through the DISN Connection Approval Process (CAP) to get your Authorization to Connect (ATC)**
- **Here is a slide presentation about the DISN CAP. Follow this process to get an ATC: http://disa.dtic.mil/disnvtc/dvs_connection.ppt**

THE ROOF
Prepare for DISN Connectivity
THIRD LEVEL
Step VI: Accreditation
SECOND LEVEL
Step V: Complete All DIACAP Documentation
Step IV: Develop a Scorecard
FIRST LEVEL
Step III: Secure the System
FOUNDATION
Step II: Document the System
Step I: Plan the DIACAP

DISA
A Combat Support Agency

What's Next?

- **Maintain IA Posture**
  - **Review of IA Controls must occur at least annually**
  - **Use DISA and other tools to keep VTF secure**
- **Initiate Re-Accreditation**
- **Retire System**

DISA
A Combat Support Agency

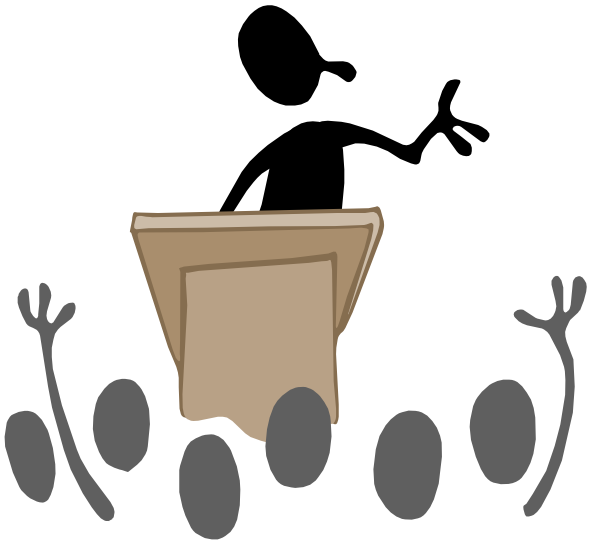
References

- **For current and future ISDN & IP VTF customers: Everything you need for the VTF DIACAP Process is available at the VTF DIACAP Web Site:**
  - **http://www.disa.mil/disnvtc/diacap.htm**
- **VTF DIACAP Scorecard Matrix**
  - **http://www.disa.mil/disnvtc/scorecard.htm**
- **DISA STIG Security Checklists are available from:**
  - **http://iase.disa.mil/stigs/checklist/index.html**
- **If you still have questions, contact the DISN Customer Contact Center (DCCC):**
  - **Commercial (614) 692-4790, option 4**
  - **Toll Free Commercial (800) 554-DISN (3476), option 4**
  - **DSN (312) 850-4790, option 4**
  - **Global DSN (510) 376-3222, option 4**
  - **DCCC@csd.disa.mil**

DISA

A Combat Support Agency

Questions?



www.disa.mil